CAN YOU BE READY FOR A THREAT YOU DON'T KNOW ABOUT?

The Art of Zero-Day Threat Coverage

TREND MICRO™

Unknown threats. Very real risks.

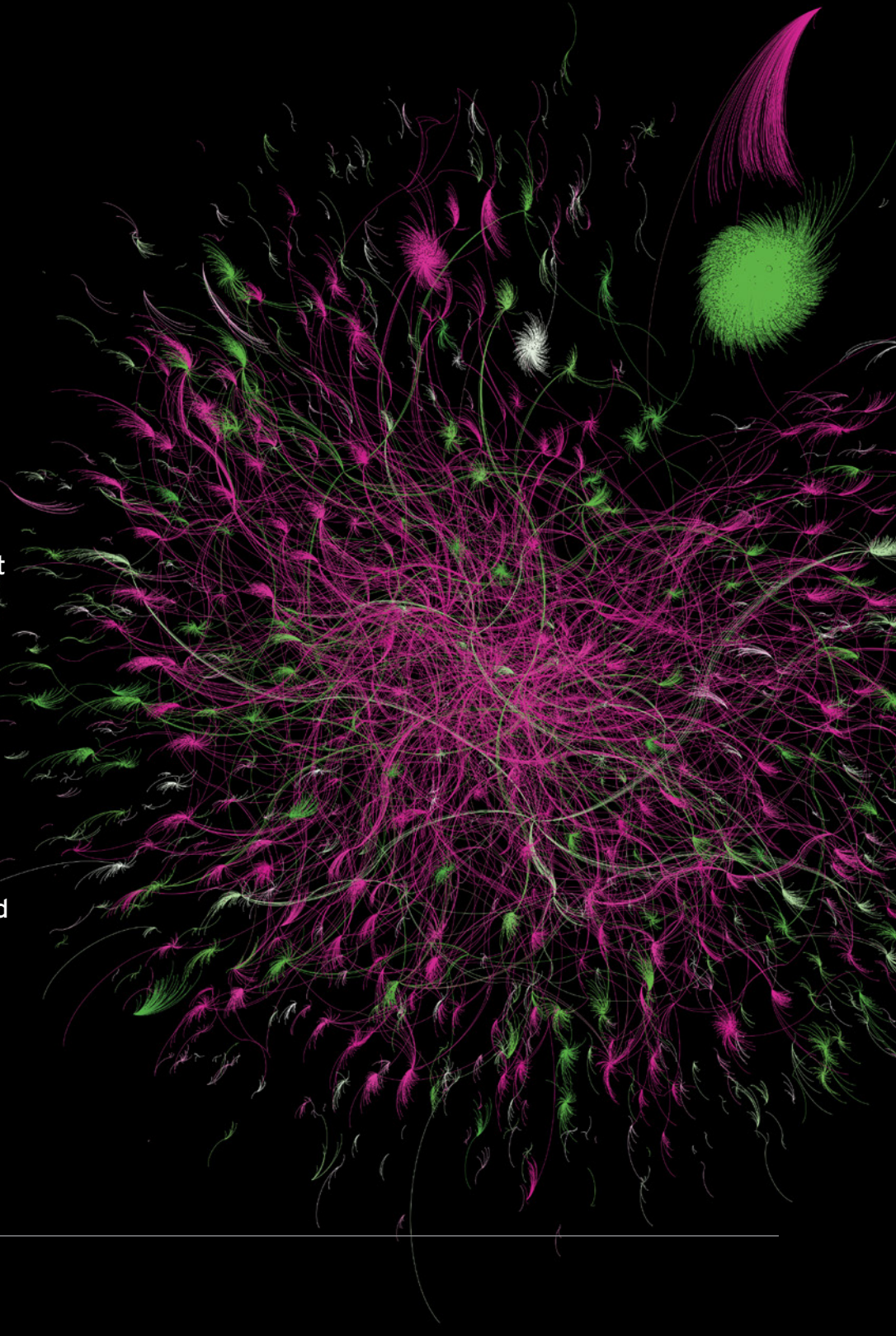
In the network security world, threats can be known—or unknown. Among the unknown kind are **zero-day threats:** ones that have already been used in a real attack but have yet to be publicly disclosed by the software vendor. In the time between the threat's discovery ("day zero") and its disclosure, enterprises are completely in the dark about the risks they might be facing.

While security vendors have been discussing zero-day threats a lot as of late, many use "zero day" as a blanket term to describe any type of threat that has not yet been disclosed but is being used by malicious operators. **Painting in such broad strokes, however, leaves enterprises vulnerable.**

There are actually three different types of zero-day threats enterprises need to know about:

- **Zero-day vulnerabilities**
- **Zero-day exploits**
- **Zero-day malware**

Each one requires **an artist's touch** to provide proactive and efficient network defense



VULNERABILITIES PROTECTED
This artwork represents 10 years of automated protection delivery for 22,500 different vulnerabilities, including 1,854 where Trend Micro provided protection 70+ days earlier than a patch. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**

ZERO-DAY VULNERABILITIES
The truly invisible threat.

When most security vendors talk about zero-day threats, they're usually referring to software and system vulnerabilities that have been newly discovered but not yet disclosed to the general public. But that can take days or even weeks—and a patch release can take even longer. In the meantime, that vulnerability presents a ripe target for attackers. That's because **software vendors often aren't the only ones aware of zero-day vulnerabilities.**

In some cases, the researchers who discover the vulnerabilities sell the information to cybercriminals, who then race to exploit the weakness before it is disclosed and patched. Even though zero-day vulnerabilities can be relatively short-lived, the brief time before they become "known" can feel like an eternity given the risks they present to enterprises.

The best way to address zero-day vulnerabilities is with an approach to network defense that's one step ahead of the software vendor.

THE ARTIST AT WORK

How Trend Micro handles zero-day vulnerabilities

The work of independent security researchers is essential to defending against zero-day vulnerabilities. Through "bug bounty" programs, researchers are rewarded for identifying and responsibly disclosing vulnerabilities before they can be exploited—and our Trend Micro™ **Zero Day Initiative™ (ZDI)** is the largest program in the world.

Concurrent to our reporting the vulnerability to the vendor, we take what researchers have shared with the ZDI to quickly develop and distribute security filters for our Trend Micro™ **TippingPoint™ Threat Protection System (TPS).** These filters cover an entire vulnerability, ensuring our customers are proactively protected before the vendor's patch is made available. In 2018, ZDI filters were distributed an average of 61 days ahead of vendor patch.

The ZDI is the global leader in vulnerability research and discovery, publishing more than 5,500 vulnerability advisories since 2005. It is a top provider of vulnerabilities to organizations like Adobe, Microsoft® and the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Without the ZDI, many vulnerabilities would remain behind closed doors or be sold on the black market for nefarious purposes.

WHAT IS A VULNERABILITY?

A vulnerability refers to any weakness in software, operating systems or devices—such as buffer overflows, missing data encryption, or a lack of authorization required for critical functions—that can be exploited to allow unauthorized access, elevation of privileges or denial of service. **A tool used to attack a vulnerability is called an exploit.**

ZERO-DAY EXPLOITS
New twists on old classics.

An exploit is code written specifically to take advantage of a vulnerability. A single vulnerability could have hundreds of exploits targeting it, each using a variation of a common technique (one will inject code using a Word file, another might use Excel). When an attacker comes up with an entirely new way to leverage a known vulnerability, that's called a **zero-day exploit.**

Until the software vendor publicly acknowledges or releases a patch that mitigates either the full scope of the targeted vulnerability or the specific technique used by the zero-day exploit, **only the person who wrote the exploit knows it exists.** And that makes it hard to stop that person from using the exploit to install malware, remotely execute code, or worse.

Yet most exploits, new and old, take a definable path to and from an application—meaning it's possible to create rules at the network layer to prevent them from doing what they set out to do.

WHAT IS AN EXPLOIT?

An exploit is a code that, when used, allows intruders to remotely access a network and gain elevated privileges. Exploits are usually written by security researchers as a proof-of-concept threat or by malicious actors for use in their operations.

THE ARTIST AT WORK

How Trend Micro handles zero-day exploits

Exploit behavior can be detected based on the techniques, protocols and ports used to attack a vulnerability. That's why Trend Micro™ **Deep Discovery™ Inspector** analyzes more than 100 protocols and all network ports, drawing on the exploit data gathered by Trend Micro™ **Smart Protection Network™** to identify possible threats. Analyzing terabytes of data collected daily on known good and bad files, applications, IP addresses and URLs, the Smart Protection Network delivers the latest security intelligence to all our products so they can adapt to emerging threats.

This data powers the machine learning and behavioral analysis that allows for new security filters to be developed for our **TippingPoint Threat Protection System (TPS).** For example, because a command-and-control (C&C) server for a zero-day exploit will use an IP or DNS address for a very short period of time, creating a filter to block that traffic would be a short-term fix only. But by crunching the data collected by the Smart Protection Network on that vulnerability as a whole, filters can be created that block any unknown exploits using known shared paths and behaviors.

ZERO-DAY MALWARE

Malware is constantly changing.

The vast majority of malware targets and exploits known software vulnerabilities to gain elevated access privileges and infect the host system. If the malware is known to security vendors, its hash signature can be detected in transport, allowing their solutions to filter and block the malware.

But malware authors have to **change just one piece of the code to alter the entire signature**—effectively creating an all-new, unknown malware that nobody has seen before. If that new zero-day malware takes advantage of zero-day exploits or zero-day vulnerabilities (or even both), it becomes nearly undetectable by conventional means.

With an intelligent and robust approach to intrusion prevention, however, it's not completely undetectable.

THE ARTIST AT WORK

How Trend Micro handles zero-day malware

Defending against unknown and undisclosed threats such as zero-day malware requires threat research that can then be used to develop filters targeting the root cause of the vulnerability being exploited. Getting to the root cause makes it possible to detect and block a broad range of common malware behaviors and techniques rather than the exploit-specific signatures found in a single malware variation.

Our **TippingPoint Threat Protection System** ships with a comprehensive set of curated filters that cover the latest known and emerging threats. TippingPoint can also be integrated with Trend Micro™ **Deep Discovery Analyzer** to automatically send potential threats or suspicious objects to a custom sandbox for detonation and analysis. This sandbox uses a precisely-tuned virtual image that replicates an enterprise's real system configurations, including drivers, operating systems, public internet access and installed applications—tricking malware into executing itself and exposing behaviors such as multi-stage downloads and C&C communications. The findings are then shared with TippingPoint and other Trend Micro solutions to prevent further malicious activity.

HOW MALWARE WORKS

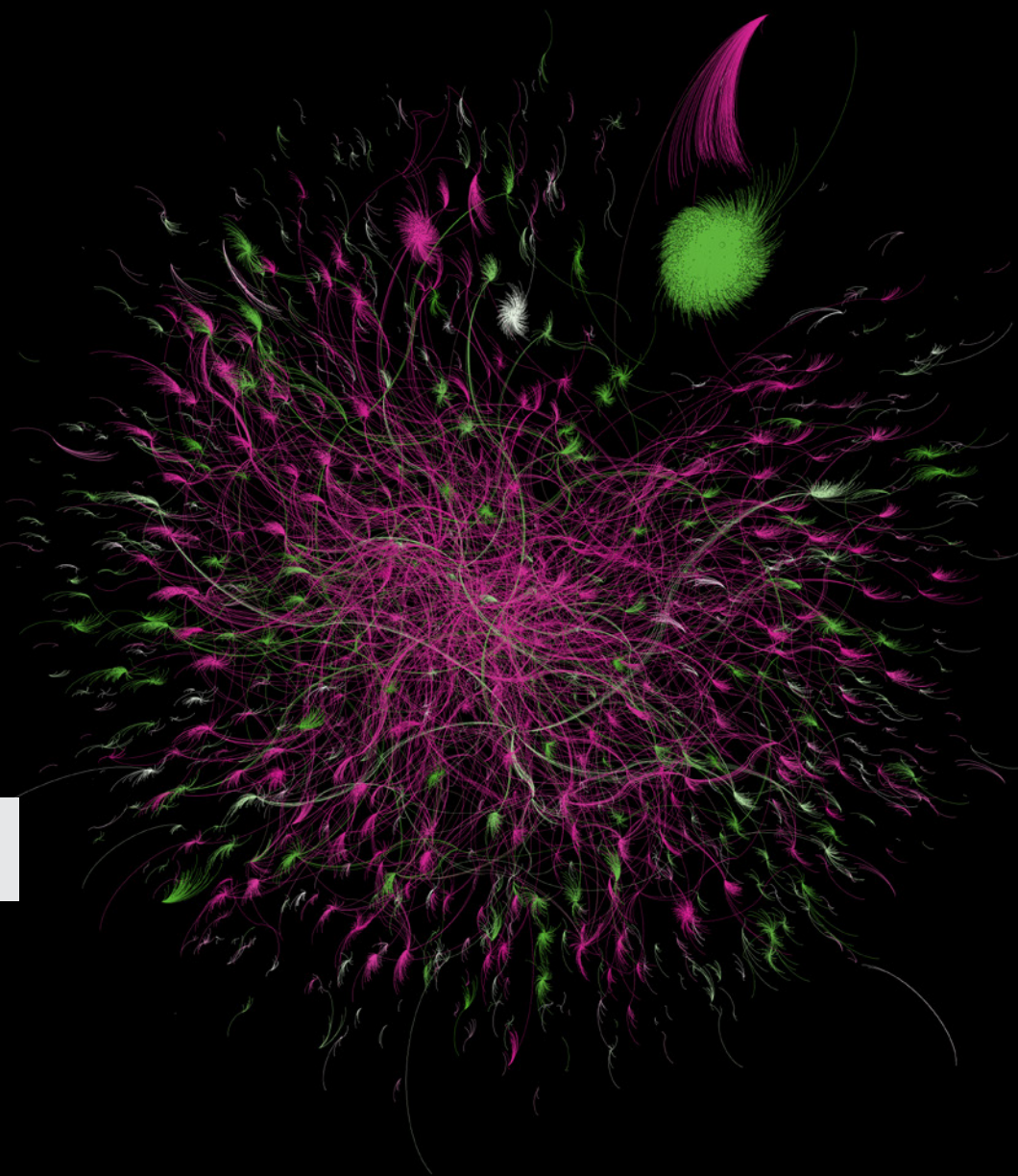
Malware is an exploit-delivery mechanism that comes as a complete software package: it infects a server or workstation, contacts a command-and-control server and pulls down a secondary payload that then detonates and spreads laterally across the network. It can take many forms, including downloadable files or embedded script on a website.

Zero-day threats can be ugly.
We make cybersecurity beautiful.

When it comes to network security, what you don't know can hurt you in the form of unknown and undisclosed threats. The ways in which businesses are targeted and attacked are constantly changing. That makes research and intelligence a vital component of any security strategy.

At Trend Micro, we know network defense tools are only as good as the data provided to them. That's why we invest so heavily in our security research capabilities. Uniquely positioned as both a security vendor and research leader—providing the intelligence that powers all of our solutions—we can provide an unmatched level of protection against known, unknown and undisclosed threats, including zero-day vulnerabilities, exploits and malware.

In the end, it's about delivering the right security at the right time.



That's the art of zero-day threat coverage.
That's the art of *cybersecurity.*

Discover the beauty in your cybersecurity solutions.
Visit www.TheArtOfCybersecurity.com to learn more.